IN THE CLAIMS:

Please AMEND claims 1, 3-8, 10, 13, 16, 17, 20, 21, 30, 31 and 34-37 as follows.

1. (Currently Amended) A method, comprising:

receiving a message from a terminal device connected to a packet data network;

deriving ~~a~~ first source information from said message;

deriving ~~a~~ second source information;

comparing said first source information and said second source information;

initiating ~~a~~ protection processing based on a result of said comparing; and

providing secure access to said packet data network based on said protection processing.

2. (Cancelled)

3. (Currently Amended) The method according to claim 1, wherein said second source information ~~is a~~comprises source address information derived from a packet data unit configured to convey said message, or from a security association set up between said terminal device and said packet data network.

4. (Currently Amended) The method according to claim 1, wherein said protection processing comprises ~~a~~ processing ~~for~~to dropping said message ~~if~~when the result

of said comparing is that said first source information and said second source information do not indicate the same location.

5. (Currently Amended) The method according to claim 1, wherein said protection processing comprises ~~a~~ processing ~~for~~to dropping said message ~~if~~when said comparing leads to the result that said first source information and said second source information do not match.

6. (Currently Amended) The method according to claim 1, wherein said first source information ~~is~~comprises an internet protocol address.

7. (Currently Amended) The method according to claim 6, wherein said message ~~is~~comprises a session initiation protocol message.

8. (Currently Amended) The method according to claim 1, wherein said second source information ~~is~~comprises at least a part of an internet protocol source address of an internet protocol datagram.

9. (Cancelled)

10. (Currently Amended) The method according to claim 3, wherein said second source information ~~is~~comprises an internet protocol address bound to an integrity key of said security association.

11. (Previously Presented) The method according to claim 10, wherein said internet protocol address is stored in a database of a proxy server configured to route said message to said packet data network.

12. (Previously Presented) The method according to claim 10, wherein said message is conveyed using a session initiation protocol level protection function.

13. (Currently Amended) An apparatus, comprising:

a receiving unit configured to receive a message from a terminal device connected to ~~said~~a network element;

a deriving unit configured to derive ~~a~~ first source information from said message, and to derive ~~a~~ second source information;

a comparing unit configured to compare said first source information and said second source information; and

a protecting unit configured to initiate ~~a~~ protection processing based on a comparing result of said comparing unit and to provide secure access to a packet data network based on said protection processing.

14. (Previously Presented) The apparatus according to claim 13, wherein said deriving unit is configured to derive said second source information from a packet data unit configured to derive said message or from a security association set up between said terminal device and said apparatus.

15. (Previously Presented) The apparatus according to claim 13, wherein said deriving unit is configured to derive said first source information from a header portion of said message.

16. (Currently Amended) The apparatus according to claim 13, wherein said protecting unit is configured to initiate ~~a~~ processing ~~for~~to dropping said message ~~if~~when said comparing result indicates that said first source information and said second source information do not indicate a same location.

17. (Currently Amended) The apparatus according to claim 13, wherein said protecting unit is configured to initiate ~~a~~ processing ~~for~~to dropping said message ~~if~~when said comparing result indicates that said first source information and said second source information do not match.

18. (Previously Presented) The apparatus according to claim 13, wherein said deriving unit is configured to read said second source information from a database provided at said apparatus.

19. (Previously Presented) The apparatus according to claim 13, wherein said deriving unit is configured to derive said second source information by extracting an internet protocol source address from an internet protocol datagram.

20. (Currently Amended) The apparatus according to claim 13, wherein said apparatus ~~is~~comprises a proxy server.

21. (Currently Amended) The apparatus according to claim 20, wherein said proxy server ~~is~~comprises a proxy call state control function of an internet protocol mobility subsystem.

22-28. (Cancelled)

29. (Previously Presented) The apparatus according to claim 14, wherein said deriving unit is configured to derive said first source information from a header portion of said message.

30. (Currently Amended) The apparatus according to claim 14, wherein said protecting unit is configured to initiate ~~a~~ processing ~~for~~to drop~~ping~~ said message ~~if~~when said comparing result indicates that said first source information and said second source information do not indicate the same location.

31. (Currently Amended) The apparatus according to claim 14, wherein said protecting unit is configured to initiate ~~a~~ processing ~~for~~to drop~~ping~~ said message ~~if~~when said comparing result indicates that said first source information and said second source information do not match.

32. (Previously Presented) The apparatus according to claim 14, wherein said deriving unit is configured to read said second source information from a database provided at said apparatus.

33. (Previously Presented) The apparatus according to claim 14, wherein said deriving unit is configured to derive said second source information by extracting an internet protocol source address from an internet protocol datagram.

34. (Currently Amended) The apparatus according to claim 14, wherein said apparatus ~~is~~comprises a proxy server.

35. (Currently Amended) The apparatus according to claim 34, wherein said proxy server ~~is~~comprises a proxy call state control function of an internet protocol mobility subsystem.

36. (Currently Amended) An apparatus, comprising:

receiving means for receiving a message from a terminal device connected to ~~saida~~ network element;

deriving means for deriving ~~a~~ first source information from said message, and for deriving ~~a~~ second source information;

comparing means for comparing said first source information and said second source information; and

protecting means for initiating ~~a~~ protection processing based on a comparing result of said comparing means and for providing secure access to a packet data network based on said protection processing.

37. (Currently Amended) A computer program embodied on a computer-readable storage medium, the computer program configured to control a processor to perform operations comprising:

receiving a message from a terminal device connected to a packet data network;

deriving ~~a~~ first source information from said message;

deriving ~~a~~ second source information;

comparing said first source information and said second source information;

initiating ~~a~~ protection processing based on a result of said comparing; and

providing secure access to said packet data network based on said protection processing.